ISO/IEC JTC 1/SC 27 N 2354

ISO/IEC JTC 1/SC 27/WG 3 N 480

REPLACES: SC 27 N 2288
WG 3 N 478

ISO/IEC JTC 1/SC 27

Information technology – Security techniques

Secretariat: DIN, Germany

DOC TYPE:	Disposition of Comments
TITLE:	Revised dispositions of NB comments on ISO/IEC WD 15446 (SC 27 N 2172), Information technology - Security techniques – Guide for production of Protection Profiles and Security Targets
SOURCE:	18th SC 27/WG 3 meeting in Madrid, Spain, April 1999
DATE:	1999-07-07
PROJECT:	1.27.22
STATUS:	This document superseds the previous version of the dispositions of comments circulated as document SC 27 N 2288 (WG 3 N 478), and is being submitted for information.
ACTION:	**FYI**
DUE DATE:	
DISTRIBUTION:	P, O and L-Members L. Rajchel, Secretariat JTC 1 K. Brannon, ITTF W. Fumy, SC 27 Chairman M. De Soete, T. Humphreys, S. Knapskog, WG-Conveners M. Donaldson, Project Editor
MEDIUM:	Server
NO. OF PAGES:	26

Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung e.V., 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: passia@ni.din.de

ISO/IEC JTC 1/SC 27/WG 3 N 480

ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - “Information Technology”
SC 27 - “Security Techniques”
WG 3 - “Security Evaluation Criteria”

TITLE: Disposition of comments - Guide for the production of PPs and STs

SOURCE: WG 3 Meeting, Madrid, Spain, 1999-04

DATE: 1999-07-01

PROJECT: ISO/IEC JTC 1.27.22

STATUS: For distribution within ISO/IEC JTC 1/SC 27

ISO/IEC JTC 1/SC 27/WG 3 N480
July 1st, 1999

Instructions for developing a further working draft of the Technical Report - Guide for the production of Protection Profiles and Security Targets

The working draft should continue to be filled in those areas which are currently covered only briefly or not at all. The following detailed points should be addressed.

1. Structure and worked examples.
   The editor is to provide any diagrams which would help to guide the PP or ST author.
   The editor is encouraged to continue with the approach adopted in the Technical Report with respect to having 'specific' product guidance as separate appendices.

2. NB comments provided in 1999-04-14 ISO/IEC JTC 1/SC 27 N2248rev1, and their disposition provided in 1999-04-23 ISO/IEC JTC 1/SC 27/WG3 N478 (this document) to be addressed during the update of the working draft.

   During the WG3 meeting there was insufficient time available to address all of the comments provided. Section 2 of this document has the detailed disposition of those discussed. Section 3 of this document has the categorisation of the comments provided, which was used to identify those comments which required more discussion.

   The remaining comments were deferred to the editor to proceed with their resolution. However, an updated disposition incorporating how all comments were addressed is to be provided with the next update of the working draft.

3. Meeting input.
   The working draft to be updated taking into account the comments provided during the WG3 sub-group and plenary during the Madrid, Spain, 1999-04 meeting. Specifically:

   - Paragraph numbers should be added to the document to facilitate review;
   - Objectives and requirements often seem to be used interchangeably, and they should not;
   - Equal weight should be given to the provision of guidance on SARs and SFRs. The current draft concentrates on the SFRs;
   - Any abbreviations used should be listed, e.g. OSP;
   - Annex C should contain a brief statement in the introduction as to why FCS is specifically called out in an annex. There might be more such annexes;

4. Further draft.
   The editor is requested to deliver a seventh working draft of the technical report in advance of the 1999-10 meeting of WG 3 to enable the working group members to review and comment prior to the meeting. The working draft to indicate that this is the seventh working draft.
   The date for such a delivery to be on or before 1999-07-01.

ISO/IEC JTC 1/SC 27/WG 3 N480
July 1st, 1999

Disposition of comments agreed during the WG3 meeting on - Guide for the production of Protection Profiles and Security Targets

German NB Comments :

General	Comment
Comment #1	Agreed. What should be described either in each rationale section OR once to describe completeness approach for all rationale sections. What needs to be described is the performance of many "iterations" of looking at the assets-threats-objectives-functions relationships. That the approach is to look for gaps in the rationale, and filling these and at this point you "assume" that it is complete. Yes, if something changes or a problem is pointed out then this must then be fixed. The final point is that the rationale required in the PP or ST should not be capable of being written if the material is incomplete.
Comment #2	Agreed. Specific comments will be addressed as appropriate. The sections on composability issues will be extracted and brought together in a single chapter at the end of the main body. It will be acknowledged that this is an area where to date there has been little practical experience. Further guidance will be provided in future versions of the PP/ST Guide as and when practical experience is gained in this area.

Detailed	Comment
Comment #1	Agreed. The original soft copy contained the appropriate identification to be added, but this appears to have been lost in the translation to PDF.
Comment #2	Agreed. There appears to be a discrepancy on bolding. The use of italics is described, however changes in fonts appear to be caused by conversion of the original soft copy of the document. The revised working draft will fully describe any use, and ensure that any conversion does not corrupt the intended approach.
Comment #3	Agreed. It should be made VERY clear in the guide that it is not the elements which have been selected. There should be a general description of how refinement can be used to rename components, and the elements within them, in order that the PP and ST author can make the text read more relevant to the product or system being documented. It should be clearly indicated what has been refined and a rationale provided as to why the changes have been made. These being required to support the evaluation of the PP or ST.

Japanese NB Comments :

Detailed	Comment
Comment #1	Not Agreed. It would appear that the comment is based on a misinterpretation of the title of Clause 3.3.3. It is that “threats” are “specified” in Section 3, and then how they are “addressed” or “handled” is given in Section 4 of the guide. There is also no intention in 15408 or the guide to define any inherent ordering of the development of the parts of a PP or ST, as the process is essentially iterative in nature. It is suggested that the title of the clause in the guide will be updated to avoid this confusion.
Comment #2	Not Agreed. There appears to be a misunderstanding here. It is assurance in the implementation of the SFRs is what is required NOT that assurance is provided BY the SFRs. This will be made clearer.
Comment #3	Agreed, but modified. There cannot be a “clear” choice for specifying which level of audit is to be specified. The sub-group felt that the PP or ST author would be required to comply with an audit policy (actual or intended). The policy can then be compared to the specification required in the CC, and the appropriate “match” used. The document contains guidance on the factors to consider, the document will be reviewed to see if any further guidance can be added.
Comment #4	Agreed, but modified. There cannot be a “clear” choice for specifying strength of function claims. The sub-group felt that the PP or ST author should state specific metrics where available (which can be considered “clear”), and that the remaining basis on which to claim a strength was built using the rationale statement. The document contains guidance on the factors to consider, the document will be reviewed to see if any further guidance can be added.
Comment #5	Agreed. The sub group agreed that a complete and comprehensive annex could never be built, however an example of how one can be constructed, and how this can aid the development of PPs and STs will be provided based on the example provided by the commentor.

French NB Comments :

General	Comment
§3.5.2, 1st para	1st Part - Agreed. This will be clarified - a full description may be provided by reference to a PP with additional details where relevant. 2nd Part - Agreed. This statement will be clarified.
§3.5.2, 3rd para	Agreed.
§5.1	Agreed. This is a specific instance where the guidance document does not give equal guidance to SARs as to SFRs. Here, and throughout the guide equal weight should be given to ALL security requirements (both functions and assurance).
§5.2.1, 1st comment	Agreed. A problem in translation to PDF resulted in the loss of Figure 4 from the original, and its substitution by a copy of Figure 3.
§5.2.1, 2nd comment	Not Agreed. See response to detailed comment #9. However, the benefits of the approach will be emphasised in a more obvious fashion.
§5.2.1, 3rd comment	Not Agreed. It is not agreed that there is any conflict between the two paragraphs.
§5.2.2	Agreed, but modified. Recommendation is that refinements are italicised/highlighted as per assignment or selection. This is not necessary for iteration since it is clear when iteration has been performed.
§5.4.3	There were 2 parts to this comment: First part - Agreed. This is a specific instance where the guidance document does not give equal guidance to SARs as to SFRs. Here, and throughout the guide equal weight should be given to ALL security requirements (both functions and assurance). Second part – Agreed. This is a misunderstanding arising from how the intended guidance is expressed. The paragraph to be reworded. The guidance is also applicable to a PP, and should be added to that part of the guide.
§8.3.8	Agreed. The TSS is an re-expression from a different perspective, and therefore any reuse of the results of the analysis would have to interpret the results from this different perspective.
B.1	Agreed.
B.4	Agreed.
Annex C	Agreed, but modified. See response to detailed comment #39
C.3.1.3	Agreed. It will be noted that these are not necessarily restricted to cryptographic assets.
Tables 10 & 11	Not Agreed. The examples are more specific, e.g. by use of the term “cryptography-related assets”. The tables could not be removed without also analysing the (potentially significant) knock-on effects.
C.4.5.7	Not Agreed. However, the 2nd paragraph will be updated to comply with the wording of Common Criteria.

C.5	Agreed, but modified. The content of this section is considered to contain useful guidance to PP/ST authors relating to the scoping of the application of assurance requirements to cryptographic functionality. The title will therefore be changed to reflect this.

Detailed	Comment
Comment #1	Not Agreed, but noted. The guide is addressing different aspects at different points in the document, which might give the impression of some duplication. The specific instances given will be checked. Possible future formats, such as HTML, is expected to help address duplication.
Comment #2	Agreed. More specific references will be provided to CC Parts 1 & 3.
Comment #3	Not Agreed. A PP may be used as a vehicle for specifying security requirements for a system. See response to other comments (e.g. Canadian comment #M1). However, the last sentence of the 1st paragraph to section 1.2 will be deleted as this is redundant and possibly confusing.
Comment #4	Agreed. This will be clarified. It will be emphasised that “conciseness” is a desirable quality to aim for when specifying security objectives; however, it is not a CC requirement against which a PP/ST will be evaluated. Security objectives will not be failed on the grounds of verbosity alone - although this of course may lead to other problems.
Comment #5	Agreed. This will be clarified. This particular guidance is only applicable when the approach is (to some extent at least) “bottom-up”, i.e. the SFRs are already known even if they haven’t yet been expressed in CC Part 2 terms. If the “classical top-down” approach is being followed then the guidance clearly does not apply.
Comment #6	Agreed. The sentence will be deleted and replaced by more appropriate guidance, reflecting the fact that an objective may address more than one threat, assumption or OSP.
Comment #7	Agreed. The missing lines are present in the original soft copy. They appear to have been lost in the process of translation to PDF.
Comment #8	Agreed. Refinement will be explained in terms consistent with CC Part 2 section 2.1.4.4.
Comment #9	Not Agreed. The footnote indicates that this distinction is purely for the purposes of the Guide only and is not part of CC. Drawing a distinction between those SFRs that directly meet the security objectives and those which play a supporting role is considered helpful when selecting SFRs (and may also aid construction of the rationale). The benefits of this approach will, however, be emphasised more clearly in this section.
Comment #10	Agreed. Figure 4 is present in the original soft copy. The figure (and its title) appears to have been lost in the translation to PDF.
Comment #11	Agreed. See response to comment #10
Comment #12	Agreed, but modified. This will be clarified. All SFRs must contribute to satisfying the security objectives - however some play a more direct role than others.
Comment #13	Agreed. More guidance on selection of SFRs from the FMT class will be given.

Comment #14	Not Agreed. Refinement is the operation which allows the modification of text, provided the author is consistent with the other technical constraints of 15408 (i.e. the technical “intent”of the component refined cannot be changed). It should be clearly indicated what has been refined and a rationale provided as to why the changes have been made. These being required to support the evaluation of the PP or ST.
Comment #15	Agreed. It will be clarified that in cases where an assurance profile has been defined the assignment of an overall assurance level has no meaning (except to the extent that the minimum assurance level can be identified).
Comment #16	Agreed. This will be clarified in section 5.1. Figure 3 is intended to show, inter alia, how the IT security requirements are derived. It will be pointed out that SOF claims are also required in the IT security requirements section of the PP/ST.
Comment #17	Not Agreed. There are 4 paragraphs in this section. It is not clear which one the comment is referring to.
Comment #18	Agreed. The missing arrow is present in the original soft copy. It appears to have been lost in translation to PDF.
Comment #19	Agreed, but modified. The reasons for the guidance will be explained. Whilst it is true that the component dependencies are the same, it may be the case that the dependencies can only be satisfied by iteration of the components on which they are dependent. The Guide authors have seen at least one case where the consequences of iteration were overlooked when the dependency analysis was performed.
Comment #20	Agreed. This will be explained. Assigning a unique number/label enables the table to demonstrate clearly precisely which SFR satisfies the dependency. It will however be stressed that this is one way of meeting the requirement, and that other methods may be equally acceptable.
Comment #21	Agreed. See response to comment #20.
Comment #22	Agreed, but modified. See response to comment #20.
Comment #23	Agreed. The sentence will be deleted.
Comment #24	Not Agreed. There was no indication of any change required.
Comment #25	Not Agreed. The guide is not restricted to Part 2, but should address all security requirements (both functions and assurance). The guide is not the mechanism to change 15408.
Comment #26	Agreed.
Comment #27	Agreed.
Comment #28	Agreed. This will be clarified. The intent is that the PP author must look at the whole picture. If component A has identified dependencies on component B, it must be shown somewhere that these dependencies are indeed satisfied if components A and B are part of the composite TOE.
Comment #29	Agreed. This will be clarified (see also response to comment #28).
Comment #30	Not Agreed. It was decided to omit the (optional) PP claims aspect from Figure 7 for the sake of simplicity. Adding this to the Figure would not add any value.
Comment #31	Agreed.

Comment #32	Not Agreed. If specific assurance measures can be identified, a single measure may address more than one requirement. In the case of ADV_RCR, it may be possible to specify the methodologies and/or tool support used to generate the evidence.
Comment #33	Not Agreed. The approach taken is consistent with that taken elsewhere in the Guide approach composability from both the point of view of the individual components and the composite TOE.
Comment #34	Agreed. This will be clarified (see also responses to comments #26 and #29).
Comment #35	Not Agreed. Whilst security objectives are highly desirable in a functional package, the Guide cannot mandate their presence when the CC does not do so.
Comment #36	Not Agreed. Annex A is considered to provide useful guidance in a concise form. See for example, US NB comment 3.3.
Comment #37	Agreed. It will be ensured that A.4.2 is consistent with 8.3.9.
Comment #38	Agreed, but modified. It was not intended to cover every single Part 2 component in Annex B but only those used to express “common or generic” requirements. However the tables will be reviewed and new examples included where appropriate (e.g. for FAU_SEL).
Comment #39	Agreed, but modified. The rationale for inclusion of Annex C will be provided in the Guide.
Comment #40	Not Agreed. Each of the example PPs and STs was produced separately from the Guide; they were not produced purely for the purposes of the Guide. The intention is to add new examples to the Guide where considered useful.
Comment #41	Agreed, but modified. This will be clarified. Such objectives contribute to countering the threats that the security features are intended to counter.

Canadian NB Comments :

General	Comment
Comment M1	Agreed, but modified. The sub group felt that specific guidance on responding to RFPs was outside the scope of the guide. However, it was agreed that : - the guide could make reference to a PP being part of an RFP (Request For Proposal) or ITT (Invitation To Tender); - the guide could make reference to a ST being part of a response to an RFP or ITT; - the ST text should be written more from the perspective of "I will provide" solution to a problem rather that "an owner" of the problem; The latter problem should be eased once more examples of STs not written by the original PP author are available.
Comment M2	Agreed. Additional guidance to be provided in the Guide as requested.
Comment M3	Agreed, but modified. New section 3 covers descriptive parts of the PP/ST. PP claims are already addressed in the ST rationale.
Comment M4	Not Agreed. PP claims are already addressed in the ST rationale.
Comment M5	Agreed. Annex A summary guidance to be updated appropriately to reflect new guidance to be provided in the main body of the Guide relating to these sections.
Comment M6	Not Agreed, but noted. Future (non-linear) versions of the Guide should address this problem.
Comment M7	Agreed.
Comment M8	Not Agreed. The Guide will continue with the approach of providing examples for different types of TOE.

Detailed	Comment
Comment T1	Not Agreed, but noted. There is currently felt to be no need to divide the Guide into two as suggested. The proposal will be borne in mind for possible future development of the Guide, e.g. when the content is relatively stable. Future (non-linear) versions of the Guide may obviate this need.
Comment T2	Not Agreed, but noted. This would lead to repitition of guidance. Future (non-linear) versions of the Guide may address this problem. obviate this need.
Comment T3	Not Agreed. The Guide should not contradict or attempt to modify the CC
Comment T4	Agreed, but modified. See response to M1.
Comment T5	Agreed, but modified. The advantages of the approach will be highlighted.
Comment T6	Agreed.

Comment T7	Not Agreed. No specific guidance is required as to how FCS is used in the FIPS 140 process, as this is considered outside the scope of the guide. 15408 is intended to be used to meet the definition in PPs and STs for many products and systems in response to RFPs and not just those submitted for FIPS 140 validation. Any reference in Annex C which implies that it is within the scope of the Guide will be removed.

United States NB Comments :

General	Comment
Comment 3.1	Agreed, but modified. Due to the number of changes required, the guide author will attempt to incorporate as many of these changes as possible – in small incremental steps. All references to CC will be modified to ISO 15408.
Comment 3.2	Agreed.
Comment 3.3	Agreed
Comment 3.4	Agreed
Comment 3.5	Agreed but modified. The Guide will be modified to include references to potential usage of functional and assurance packages in the relevant sections. Note however that practical experience is (to date) limited.
Comment 3.6	Agreed but modified. An example should be included when there is one available. At the present time the only known examples of packages are the EALs. The Guide will therefore include a pointer to the EALs as an example of an assurance package.
Comment 3.7	Agreed
Comment 3.8	Agreed. New sections on PP Introduction and TOE Description will be provided.
Comment 3.9	Agreed. A Glossary section will be included. This will reference the CC Glossary and include any new terms introduced or used by the Guide.
Comment 3.10	Agreed. Guidance will be included, bearing in mind that the subject of non-IT requirements is at the boundary of the scope of the Guide.
Comment 3.11	Agreed. The Guide will, as a minimum, acknowledge alternative legitimate approaches or viewpoints. See also response to other specific/detailed comments.
Comment 3.12	Agreed.
Comment 3.13	Agreed, but modified. Alternative formats to be provided, especially HTML, as a longer term goal.
Comment 3.14	Not Agreed, but noted The general comment appears unsubstantiated. It appears to derive from a comment made on a specific paragraph - which will be revised (see response to comment 4.4.8). However, it is agreed that any apparent TCSEC-bias should be avoided where possible.
Comment 3.15	Agreed. The worked examples will be retained, but their purpose will be more clearly explained
Comment 3.16	Agreed but modified. Part of the intent of the section on objectives was to reflect possible bottom-up approaches, especially where the objectives could be the last to be specified (written-down). The Guide will discuss the possible alternative approaches, noting that even where a bottom-up approach is taken to writing the various sections of a PP/ST, there is still an element of a "top-down" approach in the thought processes that led to the security requirements/functions. The example cited in the comment could be used both in terms of specification of threats and threats/objectives.
Comment 3.17	Agreed but modified. The current guidance will be extracted and presented in a separate chapter (at the end of the main body). It will be reviewed for validity in so doing and modified where appropriate (e.g. in line with other specific comments). The Guide will nonetheless include as requested an appropriate 'health warning', i.e. composability is a complex issue and is currently being studied.

Comment 3.18	Agreed. Additional guidance will be provided in line with the comment’s suggestion.
Comment 3.19	Agreed. The Guide will carefully delineate between IT and non-IT aspects of the environment.
Comment 3.20	Agreed.
Comment 3.21	Not Agreed. Such guidance is felt to be outside the scope of the Guide. However, a new section is included in chapter 2 to describe the PP/ST development process.
Comment 3.22	Agreed, but modified. The sub group felt that specific guidance on responding to RFPs was outside the scope of the guide. However, it was agreed that : - the guide could make reference to a PP being part of an RFP (Request For Proposal) or ITT (Invitation To Tender); - the guide could make reference to a ST being part of a response to an RFP or ITT; - the ST text should be written more from the perspective of “I will provide” solution to a problem rather that “an owner” of the problem; The latter problem should be eased once more examples of STs not written by the original PP author are available.

Detailed	Comment
Comment 4.1.1	Agreed.
Comment 4.1.2	Agreed but modified. The Guide will state that some familiarity is assumed with Parts 2 & 3 of the CC but will avoid conveying the impression that a detailed understanding of these parts is necessary before the Guide can be read. Note that Annexes B & C of Part 1 give a good overview of the PP and ST content. Familiarity with Parts 2 and 3 are not immediately necessary, but the PP/ST author will need to gain such familiarity when coming to the selection and specification of the SARs & SFRs.
Comment 4.1.3	Agreed. A brief statement will be included: the Guide may be helpful to consumers/users in directing them to the parts of a PP/ST that are most useful to them.
Comment 4.1.4	Agreed. An explanation of purpose will be provided along the lines suggested.
Comment 4.1.5	Agreed.
Comment 4.1.6	Agreed.
Comment 4.1.7	Agreed. The section will no longer be necessary following changes required by comment 4.1.2.
Comment 4.1.8	Agreed. Section 1.4 to be rewritten in the form of a ‘traditional’ executive summary as requested.
Comment 4.2.1	Agreed. There should be clear indication in the guide that there is a differentiation between the mandatory and optional parts. Optional contents will be discussed following the table. Some text added to refer to the recommended structure reflects the cost effective evaluation of PP.
Comment 4.2.2	Agreed.
Comment 4.2.3	Agreed.
Comment 4.2.4	Agreed. Same approach to that taken for PP to be taken for ST (see response to comment 4.2.1).
Comment 4.2.5	Agreed.

Comment 4.2.6	Agreed. New section on ‘audience analysis’ to be provided with text along the lines proposed.
Comment 4.2.7	Agreed. It was not the intent to contradict section 5.4.1 guidance. The wording will be amended to ensure it is not misinterpreted.
Comment 4.2.8	Agreed but modified. The Guide will point out that there may be dependencies on non-IT environment requirements, but these are not required to be a formal part of a PP/ST.
Comment 4.2.9	Agreed. Guidance on the PP Introduction will be provided in the Guide, along the lines suggested.
Comment 4.2.10	Agreed. Guidance on the TOE Description will be provided in the Guide, along the lines suggested.
Comment 4.3.1	Agreed. It was not intended to deviate from CC.
Comment 4.3.2	Agreed. (Firewalls and Intrusion Detection Systems are obvious examples of this.)
Comment 4.3.3	Agreed.
Comment 4.3.4	Agreed, but modified. The Guide will point out that other assumptions may be included, but note that formally identified assumptions need to be traced to the security objectives which uphold them. General assumptions which do not trace to security objectives may nonetheless be usefully included as part of descriptive (informative) text within a PP/ST.
Comment 4.3.5	Agreed. There is still some confusion in the section on objectives and requirements. It should be clearer the difference in approach to assumptions and objectives. The section to be revised.
Comment 4.3.6	Agreed but modified. The Guide will emphasise the importance of risk analysis whilst acknowledging that the ‘bottom-up’ approach (cf. Comment 3.16) can be equally valid. For example, the requirements may have been derived from a risk analysis without explicit threat identification. References to risk analysis texts will not, however, be included. No specific suggestions have been made, and selection of individual texts may prove controversial.
Comment 4.3.7	Agreed but modified. The Guide will point out that policy violations (negation of OSPs) should not be treated as threats (e.g. to avoid unnecessary repetition).
Comment 4.3.8	Agreed.
Comment 4.3.9	Agreed. Additional text to be included or modified as requested in the Guide. Guidance to be provided in such a way as to avoid confusion with AVA requirements.
Comment 4.3.10	Agreed. The Guide to point out that due consideration must be given to potential availability and use of automated tools by attackers.
Comment 4.3.11	Agreed, but modified. Examples will be provided by the Guide, but not based on named national organisations. Confidentiality, Integrity and Availability will be used consistent with their usage in CC. The footnote referencing [GMITS] will be retained as this was specifically requested by a reviewer of an earlier version of the Guide.
Comment 4.3.12	Agreed, but modified. The Guide will include an additional paragraph relating to non-human sources of threats.
Comment 4.3.13	Agreed.
Comment 4.3.14	Agreed but modified. Para b) to be reworded as “their protection needs, for example protection against loss of confidentiality, integrity or availability”. This is consistent with CC Part 1 section 4.1.1. Section 3.3.2 to include a more detailed discussion on attacks against the TSF and how they should be handled.

Comment 4.3.15	Agreed but modified. It was not intended for the Guide to provide a detailed tutorial on risk analysis (see the para immediately preceding section 3.1.1). The wording in para a) essentially follows CC Part 1 Section 4.3.1: the phrase "and the consequences of any damage that may be caused" was intended to convey the same meaning as "the expected magnitude of tangible loss". However this will be clarified.
Comment 4.3.16	Agreed.
Comment 4.3.17	Agreed.
Comment 4.3.18	Agreed, but modified. The term "attack method" will be used in preference to "form of attack" to ensure consistency with CC Part 1 B.2.4b).
Comment 4.3.19	Agreed.
Comment 4.3.20	Agreed. Section 3.3.2 to be expanded to discuss "high-level threats" and "detailed attacks".
Comment 4.3.21	Agreed.
Comment 4.3.22	Agreed.
Comment 4.3.23	Not Agreed. The Guide deliberately avoids recommending one option over the other - both have advantages and disadvantages. The use of mnemonic labels does appear to be by far the most popular option used by PP/ST authors; the task of the Guide is thus to warn against the dangers so that the PP/ST author will (hopefully) take heed and avoid them.
Comment 4.3.24	Agreed but modified. The Guide will acknowledge that the CC permits a PP/ST author to identify as assets that are indirectly subject to the security requirements, e.g. access credentials (CC Part 1, 4.3.1). But it will also emphasise the need to avoid needless repetition in the security environment section, bearing in mind that the value of those assets such as access credentials will only derive value from the assets which gave rise to the security requirements. Thus a threat to such 'indirect assets' may be simply viewed as just one attack method associated with a particular 'high-level' threat. The Guide will also clarify that such 'detailed threats' should (if this view is taken) be addressed in the specification of security objectives.
Comment 4.3.25	Agreed. It was not the intent to contradict CC.
Comment 4.3.26	Agreed, but modified recommendation. Principle already accepted in the Guide that threats addressed by TOE IT, TOE environment and in combination. The section to be revised to clarify that some threats may need to be included even if the TOE plays no part in countering them.
Comment 4.3.27	Agreed, see response to comment 4.3.26.
Comment 4.3.28	Agreed.
Comment 4.3.29	Agreed, see response to comment 4.3.26 (i.e. the Guide will point out that OSPs can be satisfied by the TOE IT, TOE environment, or in combination).
Comment 4.3.30	Agreed. The intent was to avoid unnecessary repetition in the PP. It is accepted that a PP author may sometimes have no choice in the matter, and so the advice will be softened.
Comment 4.3.31	Agreed but recommendation modified. The Guide will point out that OSPs may specify solution techniques.
Comment 4.3.32	Agreed but recommendation modified. The Guide will include auditing as an example, but this will not be made "the most prominent".
Comment 4.3.33	Agreed.
Comment 4.3.34	Agreed. Clarification will be provided as requested.
Comment 4.3.35	Agreed.

Comment 4.4.1	Agreed, but modified recommendation. Major problem to be addressed by recasting Introduction. It would appear that the Introduction to the section requires to be recast to ensure the reader does not get the impression that objectives contain details of the implementation. First recommendation accepted. Second recommendation accepted. Third recommendation not accepted, as unclear and confusing and not added any value. Fourth recommendation accepted, but modified. Principle accepted, section will be reworded appropriately.
Comment 4.4.2	Agreed, but modified recommendation. Addressed by recasting 4.1 Introduction. See comment 4.4.1.
Comment 4.4.3	Agreed.
Comment 4.4.4	Agreed, but modified recommendation. Addressed by recasting 4.1 Introduction. See comment 4.4.1.
Comment 4.4.5	Agreed, but modified recommendation. Addressed by recasting 4.1 Introduction. See comment 4.4.1. In addition. The concept expressed in the comment, that objectives express the extent to which the threat is to be addressed, is an important 15408 concept. This has insufficient emphasis in the guide, and therefore additional explanation should be provided.
Comment 4.4.6	Agreed, but modified recommendation. Addressed by recasting 4.1 Introduction. See comment 4.4.1. In addition. It was noted that the concept of low-level objectives should not be used. Alternative examples should be used which do express all the objectives, rather than using shorthand. There is a distinct danger that PP and ST authors will “jump” to quickly to old solutions, and that this will stifle innovation and new approaches to solving existing security problems.
Comment 4.4.7	Agreed.
Comment 4.4.8	Agreed, but modified. The paragraph will be amended to make it less obviously TCSEC-specific. The point being made is that if there are to be two distinct access control policies, it is helpful to identify two separate TOE security objectives (at least).
Comment 4.4.9	Agreed.
Comment 4.4.10	Not Agreed.
Comment 4.4.11	Agreed, but modified recommendation. The Guide (unintentionally) gives the appearance of confusing objectives and requirements. The section to be revised accordingly to keep these notions separate.
Comment 4.4.12	Agreed.
Comment 4.4.13	Agreed.
Comment 4.5.1	Agreed.
Comment 4.5.2	Agreed.
Comment 4.5.3	Agreed.
Comment 4.5.4	Agreed.

Comment 4.5.5	Agreed.
Comment 4.5.6	Agreed.
Comment 4.5.7	Agreed.
Comment 4.5.8	Agreed.
Comment 4.5.9	Agreed.
Comment 4.5.10	Agreed. The notion of partially completed operations is a useful one to highlight, and indeed has been used in a number of example PPs. The Guide to additionally explore possibilities such as transforming an assignment into a selection.
Comment 4.5.11	Agreed.
Comment 4.5.12	Not Agreed. It is not agreed that the wording imposes **any** stylistic constraints on PP/ST authors. Modifying the wording may create confusion and obscure the point being made.
Comment 4.5.13	(No Action Required)
Comment 4.5.14	Agreed.
Comment 4.5.15	Agreed.
Comment 4.5.16	Agreed.
Comment 4.5.17	(No Action Required)
Comment 4.5.18	(No Action Required for current version of the Guide)
Comment 4.5.19	(No Action Required)
Comment 4.5.20	Agreed.
Comment 4.5.21	Agreed.
Comment 4.5.22	Agreed.
Comment 4.5.23	Agreed.
Comment 4.5.24	Agreed.
Comment 4.5.25	(No Action Required)
Comment 4.5.26	Agreed.
Comment 4.5.27	Agreed but modified recommendation. The paragraph will be clarified.
Comment 4.5.28	Agreed.
Comment 4.5.29	Agreed.
Comment 4.5.30	(No Action Required)
Comment 4.5.31	(No Action Required)
Comment 4.5.32	Agreed.
Comment 4.5.33	(No Action Required)
Comment 4.5.34	Agreed
Comment 4.5.35	(No Action Required)
Comment 4.5.36	Agreed

Comment 4.5.37	(No Action Required)
Comment 4.5.38	Not Agreed. It is not clear that such a generalisation would be valid, and may obscure the specific point being made.
Comment 4.5.39	Agreed.
Comment 4.5.40	Agreed.
Comment 4.5.41	Agreed.
Comment 4.5.42	Not Agreed. The CC does not preclude the possibility of associating different assurance requirements with SFRs provided by different components of a composite TOE.
Comment 4.5.43	(No Action Required)
Comment 4.5.44	Agreed, but modified. Existing guidance will be clarified. The proposed paragraph will be included as it contains useful advice.
Comment 4.6.1	Agreed.
Comment 4.6.2	Agreed.
Comment 4.6.3	Agreed.
Comment 4.6.4	Agreed.
Comment 4.6.5	Agreed.
Comment 4.6.6	Agreed.
Comment 4.6.7	Agreed. Reference to syslog() will be removed as this is not essential to the guidance presented.
Comment 4.6.8	Agreed.
Comment 4.6.9	Agreed. This point will be clarified.
Comment 4.7.1	Agreed, but modified. The Guide will provide some advice on application notes in Chapter 2. The use of application notes to clarify specific aspects will be highlighted where appropriate in the other parts of the Guide.
Comment 4.8.1	Agreed but modified. Explanation of completed operations is not a CC requirement. *Identification* is. The Guide will be clarified - it is possible that the rationale could provide the required identification, but this will lead to duplication of information, a greatly increased scope for inconsistencies, and more expensive PP/ST evaluation.
Comment 4.8.2	Agreed. The missing lines in the Figure are present in the original soft copy, but appear to have been lost in the translation to PDF.
Comment 4.8.3	Agreed. Consistency with ISO 15408 will be ensured.
Comment 4.8.4	Agreed. ISO 15408 terminology will be used.
Comment 4.8.5	Agreed.
Comment 4.8.6	(No Action Required)
Comment 4.8.7	Agreed.
Comment 4.8.8	Agreed.
Comment 4.8.9	Agreed.

Comment 4.8.10	Agreed. The title will be modified. “satisfy” was intended to convey the same meaning as “suitability”.
Comment 4.8.11	Agreed.
Comment 4.8.12	Agreed but modified. The term “suitability” (and similar) will be used in preference to terms such as “satisfy” or “sufficient” which may be misunderstood by the reader.
Comment 4.8.13	Not Agreed. CC Part 3 gives sufficient explanation of the EALs. Attempting to describe their historical origins is unlikely to be helpful, and is in any case outside the scope of the Guide.
Comment 4.8.14	Agreed but modified. Section 3 to explain implications of considering such issues as sophisticated attacks.
Comment 4.8.15	Agreed. The possibility of the SOF requirements being justified already as part of meeting APE_REQ.1.13C will be highlighted. The last paragraph will be clarified to cater for the possibility that the assurance requirement omits AVA_SOF.1 when it should have been included.
Comment 4.8.16	Not Agreed. Attempting to describe the historical origins of the SOF levels is unlikely to be helpful, and is in any case outside the scope of the Guide.
Comment 4.8.17	Agreed.
Comment 4.8.18	(No Action Required)
Comment 4.8.19	Agreed but modified. The Guide will discuss internal consistency as a prerequisite for mutual support. The meaning of the last two sentences in the comment is unclear.
Comment 4.8.20	Not Agreed.
Comment 4.8.21	Agreed.
Comment 4.8.22	Not Agreed, but noted. The web address for the database appears to be incorrect - the database could not be accessed, and hence it was not possible to consider whether the information it provides could be used to augment the current guidance.
Comment 4.8.23	Agreed.
Comment 4.8.24	Agreed. Clarification will be provided.
Comment 4.8.25	Agreed. The point is to be clarified.
Comment 4.11.1	Agreed.
Comment 4.12.1	Agreed.
Comment 4.12.2	Not Agreed. As stated, it is only an example, and the Guide clearly points out that specific organisations may have more detailed policy rules. It is in any case unclear what specific policy on “write-up” is considered to reflect “adequate design and development”.
Comment 4.12.3	Not Agreed. Coverage of what TCSEC considers essential is not an objective of the Guide. As comment 3.14 rightly points out, it is highly desirable to avoid any appearance of bias towards TCSEC. Also, there is no component labelled FPT_TSA in the CC.

ISO/IEC JTC 1/SC 27/WG 3 **N480**
July 1st, 1999

Categorisation of Comments on PP/ST Guide Version 0.7

The following categorisation of the review comments was provided as an input to the review discussion. The detailed disposition of the comments discussed is provided above.

Comments on general structure and format of PP/ST Guide

Nature of comment #01	Review comment requests that PP/ST Guide be published in multiple formats including HTML.
US comments	3.13
CAN comments	None
French comments	None [but see #1]
Japanese comments	None
German comments	None
Response	This has been a long-term aim of the PP/ST Guide authors and we therefore support this proposal. However, there needs to be a certain degree of stability to the content of the Guide before this proposal can be progressed. It is therefore left for future development of the PP/ST Guide.

WG3 discussed the above set of comments during their meeting. See Section 2 for their disposition.

Nature of comment #02	Review comment states that the PP/ST Guide is too large with unnecessary repetition.
US comments	None
CAN comments	None
French comments	#1
Japanese comments	None
German comments	None
Response	The PP/ST Guide will be examined and any unnecessary duplication removed. The general comment concerning the size of the document is considered to be related to the (current) linear form of the guidance. It is therefore felt that the longer term move to other formats such as HTML will address this comment.

WG3 discussed the above set of comments during their meeting. See Section 2 for their disposition.

Nature of comment #03	Review comment requests that the PP/ST Guide be split into two parts, one dealing with PP guidance, the other with ST guidance. This may entail some repetition of text where commonality exists between PP and ST.
US comments	None
CAN comments	M6, T1, T2
French comments	None [#1 appears to take an opposing view]

Japanese comments	None
German comments	None
Response	It is proposed that the current structure will be maintained (subject to other comments) in the next version. However, this proposal will be considered for future development of the PP/ST Guide.

Nature of comment #04	Review comments question the inclusion of separate guidance on cryptographic functionality. In some cases the guidance appears to repeat that contained elsewhere in the PP/ST Guide. Some guidance is out of scope.
US comments	None
CAN comments	None
French comments	Annex C (general), §C.3.1.3, Tables 10 & 11, §C.4.5.7, §C.5, #39
Japanese comments	None
German comments	None
Response	Specific comments will be addressed as appropriate. The intention is to continue with the specific cryptographic guidance for the next version at least, but the content will be examined to remove any unnecessary duplication. In the longer term the need for such guidance to be provided separately will be reviewed.

Nature of comment #05	Review comments on purpose and validity of worked examples.
US comments	3.6
CAN comments	M7, M8
French comments	#40
Japanese comments	None
German comments	None
Response	The worked examples will be retained in their current form in the next version of the PP/ST Guide (they are based on actual examples, not created specifically for the PP/ST Guide). The proposals will be considered for future development of the guide. What is needed is further practical experience, particularly with respect to STs claiming compliance with an existing PP; examples to date have tended to involve the PP and ST being essentially written by the same author. A similar consideration applies to the proposal to include an example for the development of a package (US comment 3.6).

Nature of comment #06	Review comment requests that references to CC should be replaced by references to ISO 15408, and references to CC2A removed.
US comments	3.1
CAN comments	None
French comments	None
Japanese comments	None
German comments	None

Response	It is not proposed that this change be implemented at this stage. It will be considered for future versions of the PP/ST guide

WG3 discussed the above set of comments during their meeting. See Section 2 for their disposition.

Comments on specific aspects of guidance

Nature of comment #07	Review comment requests clarification of guidance, or proposes additional material to provide necessary clarification
US comments	3.2, 3.3, 3.4, 3.5, 3.7, 3.9, 3.11, 3.12, 3.15, 3.16, 3.19, 3.20, 3.21 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.8, 4.2.2, 4.2.3, 4.2.6, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.6, 4.3.7, 4.3.9, 4.3.10, 4.3.11, 4.3.12, 4.3.14, 4.3.15, 4.3.16, 4.3.17, 4.3.18, 4.3.19, 4.3.20, 4.3.21, 4.3.23, 4.3.28, 4.3.30, 4.3.31, 4.3.32, 4.3.33, 4.3.34, 4.4.7, 4.4.9, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.5.6, 4.5.7, 4.5.8, 4.5.9, 4.5.10, 4.5.11, 4.5.14, 4.5.15, 4.5.16, 4.5.18, 4.5.20, 4.5.21, 4.5.22, 4.5.23, 4.5.24, 4.5.26, 4.5.27, 4.5.28, 4.5.29, 4.5.32, 4.5.34, 4.5.36, 4.5.38, 4.5.40, 4.5.44, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7, 4.6.8, 4.6.9, 4.8.1, 4.8.2, 4.8.3, 4.8.7, 4.8.8, 4.8.9, 4.8.11, 4.8.13, 4.8.14, 4.8.15, 4.8.16, 4.8.17, 4.8.19, 4.8.20, 4.8.21, 4.8.22, 4.8.23, 4.8.24, 4.8.25, 4.11.1, 4.12.2, 4.12.3
CAN comments	T3, T5, T6
French comments	§5.2.1 (all comments), §5.2.2, §B.1, §B.4 #2, #3, #4, #5, #6, #8, #9, #12, #13, #15, #16, #17, #19, #20, #21, #22, #23, #30, #31, #32, #33, #35, #36, #37, #38, #41
Japanese comments	Comments 1, 2, 3, 4
German comments	General comment (1st para); Detailed comments (Annex B, Annex F)
Response	All requests for clarification will be addressed. Where the reviewer has provided suggested text for included, this will be studied carefully and incorporated or adapted as appropriate, i.e. to ensure: 1. Consistency with the CC 2. Technical correctness 3. Consistency with guidance elsewhere the PP/ST Guide 4. The proposed guidance is within the scope of the PP/ST Guide.

Nature of comment #08	Review comment claims inconsistency with respect to ISO 15408
US comments	4.2.1, 4.2.4, 4.3.5, 4.3.22, 4.3.25, 4.3.26, 4.3.27, 4.3.29, 4.5.42
CAN comments	None
French comments	§5.1, §5.4.3 (both comments), #14
Japanese comments	None
German comments	None

Response	All claims of inconsistency will be investigated. 1. Any actual inconsistencies will be corrected 2. Where the guidance has been misinterpreted in such a way as to conflict with the CC, the guidance will be clarified.

WG3 discussed the above set of comments during their meeting. See Section 2 for their disposition.

Nature of comment #09	Review comment disagrees with guidance, where the issue appears to be a difference of opinion as to what constitutes good or bad practice, rather than any inconsistency with ISO 15408
US comments	4.3.24, 4.4.1, 4.4.2, 4.4.4, 4.4.5, 4.4.6, 4.4.11
CAN comments	None
French comments	§8.3.8, #24, #25
Japanese comments	None
German comments	None
Response	The guidance being questioned is actually based on practical experience which the Guide authors are reluctant to discard or ignore. Within this constraint, we will nevertheless carefully consider the point of view or concern being expressed, and will attempt to accommodate this within the Guide wherever feasible.

WG3 discussed the above set of comments during their meeting. See Section 2 for their disposition.

Nature of comment #10	Review comment claims examples are too biased towards TCSEC
US comments	3.14, 4.4.8
CAN comments	None
French comments	None
Japanese comments	None
German comments	None
Response	This comment only appears (in practice) to apply to an isolated paragraph within the Guide. Annexes B to F provide many examples that are not related to standard TCSEC C2/B1 functionality. The comment is also difficult to reconcile with US comment 4.12.3 which states that the examples are incomplete with respect to TCSEC! We therefore propose to generalise the paragraph in question and also to review Annex B to determine whether there is a need for further examples to be included.

Nature of comment #11	Editorial comments
US comments	4.1.1, 4.3.8, 4.3.13, 4.3.22, 4.3.35, 4.4.3, 4.410, 4.4.13, 4.5.12, 4.5.41, 4.8.4, 4.8.10, 4.8.12, 4.12.1

CAN comments	None
French comments	#7, #10, #11, #18
Japanese comments	None
German comments	§5.2.1
Response	All editorial comments will be addressed to correct grammatical or typographical errors, or to clarify the intended meaning.

Nature of comment #12	Review comment explicitly endorses guidance
US comments	4.5.13, 4.5.17, 4.5.19, 4.5.25, 4.5.30, 4.5.31, 4.5.33, 4.5.35, 4.5.37, 4.5.43, 4.8.6, 4.8.18
CAN comments	None
French comments	None
Japanese comments	None
German comments	None
Response	The guidance will be retained as requested.

Requests for additional guidance

Nature of comment #13	Review comments on composability issues, including requests for further guidance, acknowledgement of lack of practical experience to date, etc.
US comments	3.17, 3.18, 4.2.8
CAN comments	M2
French comments	§3.5.2 (1st & 3rd paras), #26, #27, #28, #29, #34
Japanese comments	None
German comments	General comment (2nd para)
Response	Specific comments will be addressed as appropriate. The sections on composability issues will be extracted and brought together in a single chapter at the end of the main body. It will be acknowledged that this is an area where to date there has been little practical experience. Further guidance will be provided in future versions of the PP/ST Guide as and when practical experience is gained in this area.

Nature of comment #14	Review comment requests provision of guidance for descriptive (informative) parts of PP/ST (e.g. TOE description) and also PP claims section of the ST
US comments	3.8, 4.2.5, 4.2.9, 4.2.10, 4.7.1
CAN comments	M3, M4, M5
French comments	None

Japanese comments	None
German comments	None
Response	The requested guidance will be provided.

Nature of comment #15	Review comment requests the inclusion of an additional annex providing a table of threats and security objectives.
US comments	None
CAN comments	None
French comments	None
Japanese comments	#5
German comments	None
Response	Annex B contains example threats and security objectives, which will be expanded as appropriate. It is not proposed to attempt to provide any comprehensive or complete tables since this would be difficult, time consuming, possibly misleading (since new technologies and new threats are continually evolving), and would duplicate other work.

Nature of comment #16	Review comment requests expansion of guidance to cover non-IT environment requirements
US comments	3.10, 4.3.5, 4.4.11, 4.4.12, 4.5.39, 4.8.5
CAN comments	None
French comments	None
Japanese comments	None
German comments	None
Response	No significant changes are proposed to address these comments since as CC Part 1 states such requirements "are not required to be a formal part of the PP". A brief acknowledgement of CC Part 1 B.2.6b) will be included. Detailed guidance might be misconstrued leading PP/ST authors to include such information unnecessarily in a PP/ST. However, consideration will be given as to how to best handle specific TOE configuration requirements in an ST.

Nature of comment #17	Review comment requests explanation of the relationship between FCS class and FIPS 140-1 requirements
US comments	None
CAN comments	T7
French comments	None

Japanese comments	None
German comments	None
Response	It is agreed that such guidance will be useful. Investigation is needed to determine whether such guidance can be provided in the next version of the PP/ST Guide (given time/resource constraints), or whether it is left for a future version of the Guide.

WG3 discussed the above set of comments during their meeting. See Section 2 for their disposition.

Nature of comment #18	Review comments requests that guidance should reflect the situation where the ST is being written in response to an RFP
US comments	3.22
CAN comments	M1, T4
French comments	None
Japanese comments	None
German comments	None
Response	Guidance will be provided, whilst reflecting that such cases are not necessarily the norm.

WG3 discussed the above set of comments during their meeting. See Section 2 for their disposition.